# ELLIPTIC CURVES OF RANK 1 SATISFYING THE 3-PART OF THE BIRCH AND SWINNERTON-DYER CONJECTURE

DONGHO BYEON

**Abstract.** Let $E$ be an elliptic curve over $\mathbb{Q}$ of conductor $N$ and $K$ be an imaginary quadratic field, where all prime divisors of $N$ split. If the analytic rank of $E$ over $K$ is equal to 1, then the Gross and Zagier formula for the value of the derivative of the $L$-function of $E$ over $K$, when combined with the Birch and Swinnerton-Dyer conjecture, gives a conjectural formula for the order of the Shafarevich-Tate group of $E$ over $K$. In this paper, we show that there are infinitely many elliptic curves $E$ such that for a positive proportion of imaginary quadratic fields $K$, the 3-part of the conjectural formula is true.

## 1. Introduction

Let $E$ be an elliptic curve over $\mathbb{Q}$ of conductor $N$, $X_0(N)$ the modular curve of level $N$ and $\phi : X_0(N) \to E$ a surjective morphism. Let $K$ be an imaginary quadratic field with fundamental discriminant $D_K$, where all prime divisors of $N$ split and $Cl(K)$ the ideal class group of $K$. Let $\mathcal{O}_K$ be the ring of integers of $K$ and $\mathbf{a}$ an ideal of $\mathcal{O}_K$. Then we can define the *Heegner point* on $X_0(N)$ with coordinates $j(\mathbf{a})$, $j(\mathbf{n}^\tau \mathbf{a})$, where $(N) = \mathbf{n} \cdot \mathbf{n}^\tau$ in $K$ and $\tau$ is the complex conjugation. We denote it by

$$(\mathcal{O}_K, \mathbf{n}, [\mathbf{a}]),$$

where $[\mathbf{a}]$ denotes the ideal class of $K$ containing $\mathbf{a}$. Following Birch, Stephens [B-S] and Gross [Gr], let

$$P_E^*(D_K, 1, 1) := \sum_{[\mathbf{a}] \in \mathrm{Cl}(K)} \phi((\mathcal{O}_K, \mathbf{n}, [\mathbf{a}])) \; - \sum_{[\mathbf{a}] \in \mathrm{Cl}(K)} \phi((\mathcal{O}_K, \mathbf{n}, [\mathbf{a}])^\tau).$$

Then we have

$$P_E^*(D_K, 1, 1) \in E(K).$$

Kolyvagin [Ko] proves that if $P_E^*(D_K, 1, 1)$ has infinite order, then $E(K)$ has rank 1 and the Shafarevich-Tate group $\text{III}(E/K)$ of $E$ over $K$ is finite.

Gross and Zagier [G-Z] obtain a formula for the value of the derivative of the $L$-function of $E$ over $K$ in terms of the height of $P_E^*(D_K,1,1)$. This formula, when combined with the conjecture of Birch and Swinnerton-Dyer, gives the following conjectural formula for the order of $\text{III}(E/K)$.

**Conjecture** *Assume that $D_K \neq -3, -4$. If $P_E^*(D_K,1,1)$ has infinite order, then*

$$|\text{III}(E/K)| = \Big(\frac{[E(K) : \mathbb{Z}P_E^*(D_K,1,1)]}{c \cdot \prod_{q|N} c_q}\Big)^2,$$

*where $c$ is the Manin constant of the modular parametrization $\phi$ of $E$ and $c_q$, where $q|N$ is prime, is the index in $E(\mathbb{Q}_q)$ of the subgroup $E_0(\mathbb{Q}_q)$ of points which have nonsingular reduction modulo $q$.*

In this paper, we construct infinitely many elliptic curves $E$ such that for a positive portion of imaginary quadratic fields $K$, $P_E^*(D_K,1,1)$ has infinite order and the order of the 3-primary part of $\text{III}(E/K)$ satisfies the conjectural formula. More precisely we have the following theorem.

**Theorem 1.1.** *There are infinitely many elliptic curves $E$ of conductor $N = pq$ where $p$ and $q$ are distinct primes, with distinct $j$-invariants such that for at least $\frac{1}{8} \cdot \frac{pq}{(p+1)(q+1)}$ of imaginary quadratic fields $K$, $P_E^*(D_K,1,1)$ has infinite order and*

$$\text{ord}_3|\text{III}(E/K)| = 2\text{ord}_3\Big(\frac{[E(K) : \mathbb{Z}P_E^*(D_K,1,1)]}{c \cdot \prod_{q|N} c_q}\Big) = 0.$$

In [Ja], James constructs some finite number of elliptic curves $E$ such that for a positive proportion of imaginary quadratic fields $K$, $E$ has analytic rank zero over $K$ and in [Ja1], he proves that these elliptic curves $E$ satisfy a conjectural formula, following from the Birch and Swinnerton-Dyer conjecture, for the order of $\text{III}(E/K)$ at 3. Recently we [B-J-K] found infinitely many elliptic curves $E$ such that for a positive proportion of imaginary quadratic fields $K$, $E$ has analytic rank one over $K$. This gives evidence for a conjecture of Goldfeld [Go] on the analytic rank of $E$ over $K$. However, for the order of $\text{III}(E/K)$ when $E$ has analytic rank one over $K$, much less is known except the first example in this direction $E = X_0(11)$ for the 5-part of the Shafarevich-Tate group, which is studied by Gross [Gr] and Mazur [Ma1].

## 2. Preliminaries

Let $E$ be an elliptic curve over $\mathbb{Q}$ of conductor $N$. Let $F$ be the associated newform, and for $d|N$ let $\omega_d = \pm 1$ be such that $W_d F = \omega_d F$, where $W_d$ is the Atkin-Lehner involution.

Let $p$ and $q$ be distinct prime numbers such that $p \neq 3$ and $q \equiv -1 \pmod 9$. Let $E^{pq}$ be an optimal elliptic curve over $\mathbb{Q}$ of conductor $pq$ satisfying the following conditions:
(i) $\omega_p = -1$, i.e, $E^{pq}$ has split multiplicative reduction at $p$ and $\omega_q = 1$, i.e, $E^{pq}$ has non-split multiplicative reduction at $q$.
(ii) $E^{pq}$ has a $\mathbb{Q}$-rational 3-torsion point.
Such a curve exists thanks to [p. 75, B-J-K].

In [Theorem 1.3 and Proposition 3.1, B-J-K], we prove the following proposition.

**Proposition 2.1.** *Let $K$ be an imaginary quadratic field satisfying*
*(i) $p$ and $q$ split in $K$,*
*(ii) 3 does not divide the class number of $K$,*
*(iii) $E^{pq}$ has no other $K$-rational torsion points besides $\mathbb{Q}$-rational 3-torsion points.*
*Then the Heegner point $P_E^*(D_K, 1, 1) \in E^{pq}(K)$ has infinite order.*

Now we recall the result of Nakagawa and Horie [N-H] which is a refinement of the result of Davenport and Heilbronn [D-H]. Let $m$ and $N$ be two positive integers satisfying the following condition:

> $(*)$ If an odd prime number $p$ is a common divisor of $m$ and $N$, then $p^2$ divides $N$ but not $m$. Further if $N$ is even, then (i) 4 divides $N$ and $m \equiv 1 \pmod 4$, or (ii) 16 divides $N$ and $m \equiv 8$ or $12 \pmod{16}$.

For any positive real number $X > 0$, we denote by by $S_-(X)$ the set of negative fundamental discriminants $D > -X$, and put

$$S_-(X, m, N) := \{D \in S_-(X) \mid D \equiv m \,(\mathrm{mod\ N})\}.$$

**Proposition 2.2.** *(Nakagawa and Horie) Let $D < 0$ be a negative fundamental discriminant and $r_3(D)$ be the 3-rank of the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$. Then for any two positive integers $m, N$ satisfying (∗),*

$$\lim_{X\to\infty} \sum_{D\in S_-(X,m,N)} 3^{r_3(D)} \Big/ \sum_{D\in S_-(X,m,N)} 1 = 2.$$

From Proposition 2.2 and the following fact

$$\sum_{\substack{D\in S_-(X,m,N)\\ r_3(D)=0}} 3^{r_3(D)} + 3\Big( \sum_{D\in S_-(X,m,N)} 1 - \sum_{\substack{D\in S_-(X,m,N)\\ r_3(D)=0}} 3^{r_3(D)}\Big)$$
$$\leq \sum_{D\in S_-(X,m,N)} 3^{r_3(D)},$$

we can easily obtain the following lemma.

**Lemma 2.3.** *Let $D < 0$ be a negative fundamental discriminant and $h(D)$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$. Then for any two positive integers $m, N$ satisfying (∗),*

$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_-(X,m,N) \mid h(D) \not\equiv 0 \text{ (mod 3)}\}}{\sharp S_-(X,m,N)} \geq \frac{1}{2}.$$

## 3. 3-part of the Shafarevich-Tate group

**Proposition 3.1.** *Let $K(\neq \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field satisfying*
*(i) $p$ and $q$ split in $K$,*
*(ii) 3 does not divide the class number of $K$,*
*(iii) $E^{pq}$ has no other $K$-rational 3-torsion points besides $\mathbb{Q}$-rational 3-torsion points.*
*Then* $\text{Ш}(E^{pq}/K)[3] = 0$.

**Proof:** Since $E^{pq}$ has a $\mathbb{Q}$-rational 3-torsion point, the composition factors of $E^{pq}[3]$ are $\mathbb{Z}/3\mathbb{Z}$ and $\mu_3$, so from the long exact sequence of Galois cohomology, we have the following exact sequence

$$0 \to H^1(G_{\bar{K}/K}, \mathbb{Z}/3\mathbb{Z}) \to H^1(G_{\bar{K}/K}, E^{pq}[3]) \to H^1(G_{\bar{K}/K}, \mu_3). \qquad (1)$$

For a finite set $S$ of places of $K$, we define

$$H^1(G_{\bar{K}/K}, M\,;\,S) := \{\xi \in H^1(G_{\bar{K}/K}, M)\,|\,\xi \text{ is unramified outside } S\}.$$

Then from (1), we have the following exact sequence

$$0 \to H^1(G_{\bar{K}/K}, \mathbb{Z}/3\mathbb{Z}\,;\,S) \to H^1(G_{\bar{K}/K}, E^{pq}[3]\,;\,S) \to H^1(G_{\bar{K}/K}, \mu_3\,;\,S). \quad (2)$$

Let $S^{(3)}(E^{pq}/K)$ be the 3-Selmer group of $E^{pq}$ over $K$. From [Corollary 4.4 Ch X, Si], we know that

$$S^{(3)}(E^{pq}/K) \subseteq H^1(G_{\bar{K}/K}, E^{pq}[3]\,;\,S_1)$$

where $S_1$ is the set of places of $K$ containing the infinite place and the finite places dividing $3pq$.

Let $\nu_3$ be a place of $K$ which divides 3. From the condition (iii), $E^{pq}(K)[3]$ injects in $\tilde{E_{\nu_3}}$, where $\tilde{E_{\nu_3}}$ is the reduction of $E$ modulo $\nu_3$ (see [Example 6.1.1, Ch IV, Si]). This implies that $S^{(3)}(E^{pq}/K)$ is unramified at $\nu_3$, since $E^{pq}/K$ has good reduction at $\nu_3$ (see [proof of Proposition 4.1, Ch VII, Si]). So we have that

$$S^{(3)}(E^{pq}/K) \subseteq H^1(G_{\bar{K}/K}, E^{pq}[3]\,;\,S_2)$$

where $S_2$ is the set of places of $K$ containing the infinite place and the finite places dividing $pq$.

Let $c_q$ be the index in $E^{pq}(\mathbb{Q}_q)$ of the subgroup $E_0^{pq}(\mathbb{Q}_q)$ of points which have nonsingular reduction modulo $q$. Then $c_q$ is equal to 1 or 2 because $\omega_q = 1$ (see [Theorem 14.1 (d) Appendix C, Si]). From [Proposition 3.2, S-S], we know that

$$S^{(3)}(E^{pq}/K) \subseteq H^1(G_{\bar{K}/K}, E^{pq}[3]\,;\,S_3)$$

where $S_3$ is the set of places of $K$ containing the infinite place and the finite places dividing $p$.

Let $\mathcal{O}_K^S := \{a \in K\,|\,\nu(a) \geq 0 \text{ for all places } \nu \text{ of } K,\ \nu \notin S\}$ be the ring of $S$-integers of $K$ and $Cl^S(K)$ the $S$-ideal class group of $K$; it is the factor group of the ideal class group $Cl(K)$ of $K$ by its subgroup generated by classes of primes in $S$. We note that the order of $Cl^S(K)$ divides the class number of $K$. By class field theory, we have

$$H^1(G_{\bar{K}/K}, \mathbb{Z}/3\mathbb{Z}\,;S) = \mathrm{Hom}(Cl^S(K), \mathbb{Z}/3\mathbb{Z}).$$

So if 3 does not divide the class number of $K$, then $H^1(G_{\bar{K}/K}, \mathbb{Z}/3\mathbb{Z}\,;\, S) = 0$. From (2), we have the following exact sequence

$$0 \to H^1(G_{\bar{K}/K}, E^{pq}[3]\,;\, S) \to H^1(G_{\bar{K}/K}, \mu_3\,;\, S).$$

Thus we have that

$$S^{(3)}(E^{pq}/K) \subseteq H^1(G_{\bar{K}/K}, \mu_3\,;\, S_3).$$

Since

$$H^1(G_{\bar{K}/K}, \mu_3\,;\, S_3) \cong \{b \in K^*/K^{*3} \mid \mathrm{ord}_\nu(b) \equiv 0 \pmod 3 \text{ for all } \nu \notin S_3\},$$

we have that

$$\dim_3 S^{(3)}(E^{pq}/K) \leq 2,$$

where $\dim_3$ denotes the dimension of an $\mathbb{F}_3$-vector space.

From Proposition 2.1, we know that if $K$ satisfies the above three conditions, then the Heegner point $P_E^*(D_K, 1, 1) \in E^{pq}(K)$ has infinite order and $E^{pq}(K)$ has rank 1.

$$E^{pq}(K)/3E^{pq}(K) \cong (\mathbb{Z} \oplus E^{pq}(K)_{\mathrm{tor}})/\,3(\mathbb{Z} \oplus E^{pq}(K)_{\mathrm{tor}}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Thus from the following exact sequence

$$0 \to E^{pq}(K)/3E^{pq}(K) \to S^{(3)}(E^{pq}/K) \to \mathrm{III}(E^{pq}/K)[3] \to 0.$$

we have that

$$S^{(3)}(E^{pq}/K) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \text{ and } \mathrm{III}(E^{pq}/K)[3] = 0.$$

□

## 4. Proof of Theorem 1.1

**Proposition 4.1.** *Let $K$ be an imaginary quadratic field satisfying*
*(i) $p$ and $q$ split in $K$,*
*(ii) 3 does not divide the class number of $K$,*
*(iii) $E^{pq}$ has no other $K$-rational 3-torsion point than $\mathbb{Q}$-rational 3-torsion points.*

*Let $j(E^{pq})$ be the $j$-invariant of $E^{pq}$ and $\nu_p$ be a finite place dividing $p$. Assume that* $\mathrm{ord}_3(\mathrm{ord}_{\nu_p}(j(E^{pq}))) = 1$. *Then*

$$\mathrm{ord}_3\Big(\frac{[E^{pq}(K) : \mathbb{Z}P_E^*(D_K,1,1)]}{c \cdot c_p \cdot c_q}\Big) = 0.$$

**Proof:** In [Proposition 3.1, B-J-K], to prove that $P_E^*(D_K,1,1) \in E^{pq}(K)$ has infinite order, we show that $P_E^*(D_K,1,1)$ is not trivial in $E_{D_K}^{pq}(\mathbb{Q})/3E_{D_K}^{pq}(\mathbb{Q})$, where $E_{D_K}^{pq}$ is the quadratic twist of $E^{pq}$. We note that $E_{D_K}^{pq}(\mathbb{Q})$ is the (-)-eigenspace of $\sigma \neq 1$ in $\mathrm{Gal}(K/\mathbb{Q})$ acting on $E^{pq}(K)$. We also note that $\mathrm{rank}\, E^{pq}(\mathbb{Q}) = 0$, since $\mathrm{rank}\, E_{D_K}^{pq}(\mathbb{Q}) + \mathrm{rank}\, E^{pq}(\mathbb{Q}) = \mathrm{rank}\, E^{pq}(K) = 1$. This implies that

$$\mathrm{ord}_3([E^{pq}(K) : \mathbb{Z}P_E^*(D_K,1,1)]) = \mathrm{ord}_3|E^{pq}(K)_{\mathrm{tor}}| = 1.$$

Since $E^{pq}$ is optimal and its conductor $pq$ is square-free, $c = 1$ (See [Corollary 4.1, Ma]). And $\mathrm{ord}_3(c_p) = 1$ because $\omega_p = -1$ and $\mathrm{ord}_3(\mathrm{ord}_{\nu_p}(j(E^{pq}))) = 1$ (See [Corollary 15.2.1 Appendix C, Si]). And $c_q = 1$ or $2$ because $\omega_q = 1$. So we have that

$$\mathrm{ord}_3(c \cdot c_p \cdot c_q) = 1$$

and we complete the proof. □

*Proof of Theorem 1.1:* Let $E' : y^2 + a_1xy + a_3y = x^3$, $a_1, a_3 \in \mathbb{Z}$. Then the point $(0,0) \in E'(\mathbb{Q})$ is a 3-torsion point. In [B-J-K], using a result of the binary Goldbach problem for polynomials, we show that there are infinitely many elliptic curves $E'^{pq} : y^2 + a_1xy + a_3y = x^3$, $a_1, a_3 \in \mathbb{Z}$ of discriminant $\Delta = a_3^3(a_1^3 - 27a_3) = p^3q$ and conductor $N = pq$, where $p, q$ are different primes such that $p \neq 3$, $q \equiv -1 \pmod 9$, more precisely, $q \equiv -1 \pmod{27}$ (see [Proof of Theorem 1.1, B-J-K]) and $\omega_p = -1$, $\omega_q = 1$. Let $E^{pq}$ be the optimal elliptic curve in the isogeny class of $E'^{pq}$. Since $E^{pq}$ has also a $\mathbb{Q}$-rational 3-torsion point by [Du] [Va], $E^{pq}$ can be also defined by the Weierstrass equation of the form $E^{pq} : y^2 + b_1xy + b_3y = x^3$, $b_1, b_3 \in \mathbb{Z}$ of discriminant $\Delta = b_3^3(b_1^3 - 27b_3)$ (see [Table 3, Ku]). By a change of variables, we can assume that $b_1, b_3 \in \mathbb{Z}$, $b_3 > 0$ and there is no integer $u$ such that $u|b_1$ and $u^3|b_3$. Then we can see that $E^{pq} : y^2 + b_1xy + b_3y = x^3$ is a minimal Weierstrass equation for $E^{pq}$ by checking the valuation of $\Delta$ and $c_4 = b_1({b_1}^3 - 24b_3)$.

If a prime $t$ divides $b_1$ and $b_3$, then $E^{pq}$ has additive reduction at $t$. So we can assume that $b_1$ and $b_3$ are relatively prime. Then for every prime factors $t$ of $b_3$, $E^{pq}$ has split multiplicative reduction at $t$, for every prime factors $t \equiv -1 \pmod 3$ of $(b_1^3 - 27b_3)$, $E^{pq}$ has non-split multiplicative reduction at $t$, and for every prime factors $t \equiv 1 \pmod 3$ of $(b_1^3 - 27b_3)$, $E^{pq}$ has split multiplicative reduction at $t$ because the slopes of the tangent lines at the node $(-b_1^2/9, b_1^3/27) \in E^{pq}(\mathbb{F}_t)$ are $(-3b_1 \pm b_1\sqrt{-3})/6$. So the condition that $E^{pq}$ has split multiplication at $p$, i.e, $\omega_p = -1$ and $E^{pq}$ has non-split multiplication at $q$, i.e, $\omega_q = 1$ implies that $b_3 = p^r$ and $b_1^3 - 27b_3 = \pm q^s$.

If

$$\mathrm{ord}_3(\mathrm{ord}_{\nu_p}(j(E^{pq}))) = \mathrm{ord}_3(\mathrm{ord}_{\nu_p}(\frac{b_1^3({b_1}^3 - 24b_3)^3}{b_3^3(b_1^3 - 27b_3)})) = \mathrm{ord}_3(\mathrm{ord}_{\nu_p}({b_3}^{-3})) > 1,$$

then $b_3 = p^{3r'}$ and $b_1^3 - 27b_3 = \pm q^s$ is factored by

$$b_1^3 - (3p^{r'})^3 = (b_1 - 3p^{r'})(b_1^2 + 3b_1p^{r'} + 9p^{2r'}).$$

We can see that $b_1 - 3p^{r'}$ and $b_1^2 + 3b_1p^{r'} + 9p^{2r'}$ are relatively prime. So $b_1 - 3p^{r'} = \pm 1$ or $b_1^2 + 3b_1p^{r'} + 9p^{2r'} = \pm 1$. But $b_1^2 + 3b_1p^{r'} + 9p^{2r'}$ can not be equal to $\pm 1$. Suppose that $b_1 - 3p^{r'} = \pm 1$. Then $b_1 > 0$ and $b_1^2 + 3b_1p^{r'} + 9p^{2r'} > 0$. If $b_1 - 3p^{r'} = 1$, then

$$b_1^3 - 27b_3 = (3p^{r'} + 1)^3 - 27p^{3r'} = 27p^{2r'} + 9p^{r'} + 1 - 27p^{3r'} = q^s.$$

If $s$ is odd, then the left hand side of this equation is congruent to 1 modulo 9, but the right hand side of this equation is congruent to $-1$ modulo 9. So it is impossible. If $s$ is even, then we have

$$p^{2r'} + p^{r'}/3 - p^{3r'} = (q^s - 1)/27,$$

and $(q^s - 1)/27$ is an integer, since $q \equiv -1 \pmod{27}$. So $p$ should be equal to 3, but it is contraction to the condition of $E^{pq}$. Thus $b_1 - 3p^{r'}$ can not be equal to 1. Similarly, we can show that $b_1 - 3p^{r'}$ can not be equal to $-1$. Thus $\mathrm{ord}_3(\mathrm{ord}_{\nu_p}(j(E^{pq})))$ should be equal to 1.

So for the imaginary quadratic field $K$ satisfying the conditions in Proposition 3.1 and Proposition 4.1, we have that

$$\mathrm{ord}_3|\mathrm{III}(E^{pq}/K)| = 2\mathrm{ord}_3\Big(\frac{[E^{pq}(K) : \mathbb{Z}P_E^*(D_K, 1, 1)]}{c \cdot c_p \cdot c_q}\Big) = 0.$$

Now we compute the number of imaginary quadratic fields $K$ satisfying the conditions in Proposition 3.1 and Proposition 4.1. It is known that when $X \to \infty$,

$$\sharp S_-(X) \sim \frac{3X}{\pi^2}$$
$$\sharp S_-(X, m, N) \sim \frac{3X}{\pi^2 \varphi(N)} \prod_{p|N} \frac{q}{p+1},$$

where $p$ runs over all the prime divisors of $N$ and $q = 4$ if $p = 2$, $q = p$ otherwise, and $\varphi$ is the Euler function (See [Proposition 2, [N-H]). Thus from Lemma 2.3, we obtain the following estimates.

$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_-(X) \,|\, h(D) \not\equiv 0 \,(\mathrm{mod}\ 3),\, (\frac{D}{p}) = 1 \text{ and } (\frac{D}{q}) = 1\}}{\sharp S_-(X)}$$
$$\geq \frac{1}{8} \cdot \frac{pq}{(p+1)(q+1)}.$$

And we know that there are only finitely many imaginary quadratic fields $K$ such that $E(K)$ has other $K$-rational 3-torsion point besides $\mathbb{Q}$-rational 3-torsion points (see [Exercise 8.17, Si]). So at least $\frac{1}{8} \cdot \frac{pq}{(p+1)(q+1)}$ of imaginary quadratic fields $K$ satisfy the conditions in Proposition 3.1 and Proposition 4.1. Thus we complete the proof of Theorem 1.1. □

**Acknowledgement** The author would like to thank the referee for his careful reading of this manuscript and making many valuable suggestions.

## References

[B-S] B. J. Birch and N. M. Stephens, *Computation of Heegner points,* in: Modular forms (Durham, 1983), 13–41, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984.

[B-J-K] D. Byeon, D. Jeon and C. H. Kim, *Rank-one quadratic twists of an infinite family of elliptic curves,* J. Reine Angew. Math., **633** (2009), 67–76.

[D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II,* Proc. Roy. Soc. London A, **322** (1971), 405–420.

[Du] N. Dummigan, *Rational torsion on optimal curves,* Int. J. Number Theory, **1** (2005), 513–531.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields,* Number Theory, Carbondale, Springer Lect. Notes **751** (1979), 108-118.

[Gr] B. H. Gross, *Heegner points on $X_0(N)$,* in: Modular forms (Durham, 1983), 87–105, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984.

[G-Z] B. H. Gross and D. Zagier, *Heegner points and derivatives of L-series,* Invent. Math. **84** (1986), 225–320.

[Ja] K. James, *L-series with nonzero central critical value,* J. Amer. Math. Soc. **11** (1998), 635–641.

[Ja1] K. James, *Elliptic curves of rank 0 satisfying the Birch and Swinnerton-Dyer conjecture mod 3,* J. Number Theory. **76** (1999), 16–21.

[Ko] V. Kolyvagin, *Euler systems,* The Grothendieck Festschrift, vol. II, Birkhäuser, Boston, MA, 1990, 435–483.

[Ku] D.S. Kubert, *Universal bounds on the torsion of elliptic curves,* Proc. London Math. Soc., **3 (33)** (1976) 193–237

[Ma] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld),* Invent. Math. **44** (1978), 129–162.

[Ma1] B. Mazur, *On the arithmetic of special values of L-functions,* Invent. Math. **55** (1979), 207–240.

[N-H] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points,* Proc. A.M.S. **104** (1988), 20 – 25.

[S-S] E. F. Schaefer and M. Stoll, *How to do a p-descent on an elliptic curve,* Trans. Amer. Math. Soc. **356** (2004), 1209-1231.

[Si] J. H. Silverman, *The arithmetic of elliptic curves,* Grad. Texts in Math. **106**, Springer-Verlag, New York, 1986.

[Va] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves,* J. Inst. Math. Jussieu **4** (2005), 281–316.

Department of Mathematics, Seoul National University, Seoul, Korea
E-mail: dhbyeon@snu.ac.kr